00/8119
ISR
5/19J (9)

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000174796 A**

(43) Date of publication of application: **23 . 06 . 00**

(51) Int. Cl **H04L 12/46**
**H04L 12/28**
**H04L 9/32**
**H04L 12/66**
**H04L 12/56**
**H04L 29/14**

(21) Application number: **10347235**

(22) Date of filing: **07 . 12 . 98**

(71) Applicant: **HITACHI LTD**

(72) Inventor: **TSUCHIYA KAZUAKI**
**NOZAKI SHINJI**

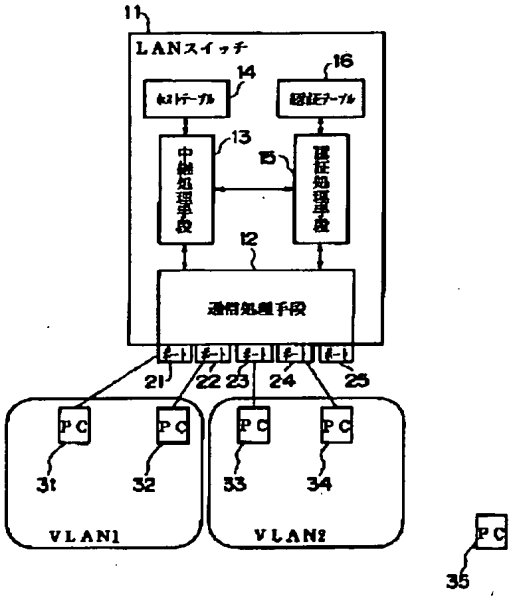
# (54) MANAGEMENT METHOD FOR COMMUNICATION NETWORK SYSTEM, AND INFORMATION REPEATER

(57) Abstract:

PROBLEM TO BE SOLVED: To facilitate the prevention of eavesdropping and impersonation by a malicious user and the analysis and restoration of an address setting error.

SOLUTION: An LAN switch 11 constitutes the communication network of a virtual LAN(VLAN) 1 and the VLAN 2, etc., by arbitrarily connecting plural personal computers(PCs) 31-34 as network terminals to respective plural ports 21-25. In this case, it is provided with a communication processing means 12 for transmitting and receiving packets with the respective ports 21-25, a relay processing means 13 for relaying the packets with the respective ports 21-25 based on a host table 14 updated by learning the change of the correspondence relation of the respective ports and the address information of the connected PC and an authentication processing means 15 for performing user authentication to the PC of a transmission origin by referring to an authentication table 16 and permitting the rewrite of the host table 14 and the relay of the packet only in the case of a true user at the time of the updating of the host table 14 of a packet relay trigger.





(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－174796
（P2000－174796A）
(43)公開日　平成12年６月23日(2000.6.23)

| (51)Int.Cl.' | 識別記号 | FI | | テーマコード'（参考） |
|---|---|---|---|---|
| H04L 12/46 | | H04L 11/00 | 310C | 5J104 |
| 12/28 | | 9/00 | 675A | 5K030 |
| 9/32 | | 11/20 | B | 5K033 |
| 12/66 | | | 102D | 5K035 |
| 12/56 | | 13/00 | 311 | 9A001 |

審査請求　未請求　請求項の数３　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願平10－347235

(22)出願日　平成10年12月７日(1998.12.7)

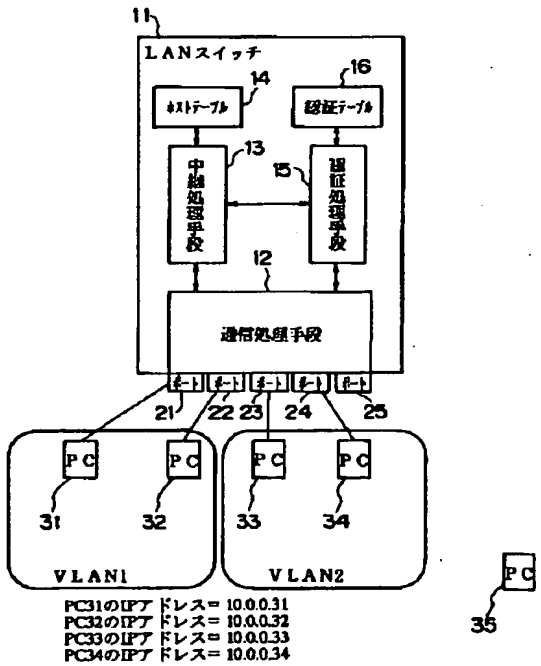
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　土屋　一暁
神奈川県海老名市下今泉810番地　株式会社日立製作所サーバ開発本部内
(72)発明者　野崎　信司
神奈川県海老名市下今泉810番地　株式会社日立製作所サーバ開発本部内
(74)代理人　100080001
弁理士　筒井　大和

最終頁に続く

(54)【発明の名称】　通信ネットワークシステムの管理方法および情報中継装置

(57)【要約】
【課題】　悪意のユーザによる盗聴やなりすましの防止、アドレス設定ミスの解析や回復を容易にする。
【解決手段】　複数のポート２１～２５の各々に任意にネットワーク端末としての複数のＰＣ３１～３４を接続することでＶＬＡＮ１およびＶＬＡＮ２等の通信ネットワークを構成するＬＡＮスイッチ１１において、各ポート２１～２５との間でパケットの送受信を行う通信処理手段１２と、各ポートと、接続されたＰＣのアドレス情報との対応関係の変化を学習して更新されるホストテーブル１４に基づき各ポート２１～２５間のパケットの中継を行う中継処理手段１３と、パケット中継契機のホストテーブル１４の更新時に、認証テーブル１６を参照して送信元のＰＣに対してユーザ認証を行い、真正のユーザの場合にのみホストテーブル１４の書き換えおよびパケットの中継を許可する認証処理手段１５とを備えた。

図　1



1

【特許請求の範囲】

【請求項１】　ネットワーク端末またはネットワーク中継装置が接続される複数の入出力ポートと、個々の前記入出力ポートと前記ネットワーク端末またはネットワーク中継装置に付与されたネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方を対応付けて格納する制御テーブルと、前記制御テーブルに基づいて複数の前記入出力ポートの各々に接続された前記ネットワーク端末またはネットワーク中継装置の相互間での通信情報の授受を行うとともに、前記通信情報に含まれる前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と前記入出力ポートとの対応関係の変化を学習して前記制御テーブルを更新することで、前記入出力ポートに対する前記ネットワーク端末またはネットワーク中継装置の接続状態の動的な変更を可能にする中継処理手段とを含む情報中継装置を用いた通信ネットワークシステムの管理方法であって、

個々のネットワーク端末に対応した前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と、当該ネットワーク端末のユーザ名およびパスワードとが対応付けて格納された認証テーブルを設定する第１のステップと、

前記制御テーブルの更新を伴う前記通信情報の授受が発生した時、前記通信情報の授受および前記制御テーブルの更新に先立って、前記通信情報の送信元および送信先の少なくとも一方のユーザに対して、前記ユーザ名およびパスワードの入力を要求し、入力されたユーザ名およびパスワードと前記認証テーブル内の前記ユーザ名およびパスワードと照合するユーザ認証を実行し、前記ユーザ認証に成功したときのみ前記制御テーブルの更新および前記通信情報の授受を実行し、前記ユーザ認証に失敗したときは前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄する第２のステップと、

を実行することを特徴とする通信ネットワークシステムの管理方法。

【請求項２】　請求項１記載の通信ネットワークシステムの管理方法において、

前記第１のステップでは、前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方に対して、前記ユーザおよび通信ネットワークシステムの管理者の少なくとも一方の連絡先メールアドレスも対応付けて設定し、前記第２のステップでは、前記ユーザ認証にて前記通信情報の送信元または送信先の前記ユーザから入力された前記ユーザ名を含むとともに前記制御テーブルの更新要求が発生したことを通知するメッセージを作成して該当する前記ネットワーク論理アドレスまたはネットワーク物理アドレスの前記ユーザおよび管理者の少なくとも一方の連絡先メールアドレスに対して送出する処理、

前記第２のステップでの前記ユーザ認証に失敗したとき、前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄し、さらに当該通信情報を受信した前記入出力ポートの切り離し、および当該入出力ポートから受信した全ての通信情報を廃棄する処理、

前記第２のステップでの前記ユーザ認証に失敗したとき、前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄し、さらに該通信情報の送信元の前記ネットワーク論理アドレスまたはネットワーク物理アドレスと同一の仮想ＬＡＮ（ローカル・エリア・ネットワーク）に属す全ての前記ネットワーク端末のユーザに、前記ネットワーク論理アドレスまたはネットワーク物理アドレス等の設定ミスや、悪意のユーザが他のネットワーク端末のアドレスを使って盗聴やなりすましの通信を行おうとしている可能性があることを警告するメッセージを作成して送る処理、

前記制御テーブルの更新要求発生の有無に関係なく、定期的または不定期に前記制御テーブル内に登録された前記ネットワーク論理アドレスまたはネットワーク物理アドレスのユーザに対して前記ユーザ認証を実行する処理、

の少なくとも一つの処理を実行することを特徴とする通信ネットワークシステムの管理方法。

【請求項３】　ネットワーク端末またはネットワーク中継装置が接続される複数の入出力ポートと、個々の前記入出力ポートと前記ネットワーク端末またはネットワーク中継装置に付与されたネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方を対応付けて格納する制御テーブルと、前記制御テーブルに基づいて複数の前記入出力ポートの各々に接続された前記ネットワーク端末またはネットワーク中継装置の相互間での通信情報の授受を行うとともに、前記通信情報に含まれる前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と前記入出力ポートとの対応関係の変化を学習して前記制御テーブルを更新することで、前記入出力ポートに対する前記ネットワーク端末またはネットワーク中継装置の接続状態の動的な変更を可能にする中継処理手段とを含む情報中継装置であって、

個々のネットワーク端末に対応した前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と、当該ネットワーク端末のユーザ名およびパスワードと、前記ユーザおよび通信ネットワークシステムの管理者の少なくとも一方の連絡先メールアドレスが対応付けて格納された認証テーブルと、

前記制御テーブルの更新を伴う前記通信情報の授受が発生した時、前記通信情報の授受および前記制御テーブルの更新に先立って、前記通信情報の送信元および送信先の少なくとも一方の前記ユーザに対して、ユーザ名およびパスワードの入力を要求し、入力されたユーザ名およびパスワードと前記認証テーブル内の前記ユーザ名およ

びパスワードと照合するユーザ認証を実行するとともに、前記通信情報の送信元および前記管理者の少なくとも一方の前記連絡先メールアドレスに対して前記ユーザ認証で得られた前記ユーザ名と前記制御テーブルの更新要求が発生したことを通知するメッセージを送信するとともに、前記ユーザ認証に成功したときのみ前記制御テーブルの更新および前記通信情報の授受を実行し、前記ユーザ認証に失敗したときは前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄する動作を行う制御論理と、
を備えたことを特徴とする情報中継装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、通信ネットワークシステムの管理技術および情報中継技術に関し、特に、ＬＡＮ(LAN: Local Area Network) スイッチ(Layer2 スイッチ、Layer3スイッチ等）と呼ばれるインタネットワーク装置、およびＬＡＮスイッチで構成する通信ネットワークシステム（ＬＡＮスイッチネットワークシステム）の管理方法等に適用して有効な技術に関する。

【０００２】

【従来の技術】ＬＡＮスイッチが有する特徴技術にＶＬＡＮ(VLAN: Virtual LAN) がある。ＶＬＡＮはインタネットワーク装置の物理的なポートに依存せずにＬＡＮの構築を可能にする技術であり、その形式の違いによってポートベースＶＬＡＮ、ＭＡＣ(MAC: Media Access Control）アドレスベースＶＬＡＮ、Layer3プロトコルベースＶＬＡＮ、ＩＰ(IP: Internet Protocol）サブネットベースＶＬＡＮ等の名称で知られている。

【０００３】本発明の参考技術では、例えば図７に示すＩＰサブネットベースＶＬＡＮの通信ネットワークシステムにおいて複数のポート２２１～２２５を備えたＬＡＮスイッチ２１０はＰＣ(PC: Personal Computer) ２３１からＰＣ２３３へのパケットを受信すると、パケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブル２２０を作成する。次に終点ＩＰアドレスをキーにホストテーブル２２０を参照し、該当エントリが有る場合は、該当ポートにパケットを出力する。該当エントリが無い場合は、ルーティングテーブル（図示無し）およびＡＲＰ(ARP: Address Resolution Protocol)テーブル（図示無し）を参照してネクストホップを決め、該当するホストテーブル２２０のエントリを新規に作成して、該当ポートにパケットを出力する。ＬＡＮスイッチ２１０はこのようにしてＰＣ２３１からＰＣ２３３へのパケットを中継する。

【０００４】さらにＬＡＮスイッチ２１０では、定期的にホストテーブル２２０のエントリを廃棄し、新たにパケットから学習することによって常にホストテーブル２２０のエントリを更新しているため、ＰＣが移動した場合でも移動先のポートにパケットを正しく中継することができる。すなわちＰＣは移動した場合でも移動前と同様の通信を自動的に再開することができる。

【０００５】

【発明が解決しようとする課題】しかしながら、上記参考技術には、次の技術的課題がある。

【０００６】第１の技術的課題は、ＩＰアドレス等の設定ミスに対して無防備なことである。例えばＰＣ２３２がＰＣ２３１のＩＰアドレスを誤って設定、ポート２２２に接続してしまったとする。この場合、ＬＡＮスイッチ２１０ではＰＣ２３１がポート２２１からポート２２２に移動したと判断し、そのようにホストテーブル２２０を書き換えてしまう。この結果、ＩＰアドレスを正しく使用しているＰＣ２３１が通信出来なくなる等の通信不良が発生する。また、ネットワークに接続されるＰＣの数が多い場合には、この通信不良の解析や回復には、多大の労力を要する。

【０００７】第２の技術的課題は、悪意のユーザによる盗聴やなりすましを許してしまうことである。例えばＰＣ２３５がＰＣ２３１のＩＰアドレスを設定、ポート２２５に接続したとする。この場合、ＬＡＮスイッチ２１０ではＰＣ２３１がポート２２１からポート２２５に移動したと判断し、そのようにホストテーブル２２０を書き換えてしまう。この結果、ＰＣ２３５がＰＣ２３１宛の通信データを受け取って盗聴したり、またＰＣ２３１になりすまして通信できてしまう。

【０００８】本発明の目的は、論理的あるいは物理的なネットワークアドレス等の設定ミスによる通信不良の防止や通信不良の原因解析および回復操作の迅速化が可能な通信ネットワークシステムの管理技術および情報中継技術を提供することにある。

【０００９】本発明の他の目的は、悪意のユーザによる盗聴やなりすましを防ぐことで通信ネットワークシステムのセキュリティを向上させることが可能な通信ネットワークシステムの管理技術および情報中継技術を提供することにある。

【００１０】

【課題を解決するための手段】本発明は、ＬＡＮスイッチ等の情報中継装置に備えられた複数の入出力ポートにユーザ端末や他の中継装置を接続して構築され、入出力ポートに対するユーザ端末等の接続状態の変化を学習して、入出力ポートとネットワークアドレスとの対応関係を管理する制御テーブルを更新することで、個々のユーザ端末の入出力ポートに対する接続状態を動的に変更することが可能な通信ネットワークの管理方法において、各ユーザ端末間、すなわち複数の入出力ポート間で通信情報の授受を契機とする制御テーブルの更新要求が発生した時、当該通信情報の送信元のユーザ端末に対してユーザ認証を実行し、真正のユーザであることが確認された場合にのみ、制御テーブルの更新およびそれに基づく通信情報の授受を行わせるものである。

【００１１】また、各ユーザ端末およびシステム管理者の連絡先メールアドレスを、ユーザ認証に用いられるネットワークアドレスやユーザ名、パスワード等が格納された認証テーブルの一部に登録しておき、制御テーブルの更新要求の発生時に、当該更新要求が発生したことを記したメッセージを通信情報の送信元のユーザ端末やシステム管理者等にメールで送るものである。この際、ユーザ認証の成功の有無に関係なく、当該ユーザ認証にて得られたユーザ名を当該メッセージ内に格納する。

【００１２】より具体的には、本発明は、以下の特徴を有する。

【００１３】第１の観点では、本発明は、ＬＡＮスイッチで構成する通信ネットワークシステムにおいて、ＩＰアドレス等の設定ミスによる通信不良、悪意のユーザによる盗聴やなりすましを防ぐことができるＬＡＮスイッチネットワークシステムの管理方法であって、例えば図１に示すＩＰサブネットベースＶＬＡＮの通信ネットワークシステムにおいて、（ａ）ＰＣ３１～３４はＬＡＮスイッチ１１に予めＩＰアドレスとそのユーザ名、パスワード、連絡先メールアドレスを登録し、（ｂ）ＬＡＮスイッチ１１の管理者も同様にＬＡＮスイッチ１１に予め連絡先メールアドレスを登録し、（ｃ）ＬＡＮスイッチは前記ＰＣ３１～３４および前記ＬＡＮスイッチ１１の管理者の情報を登録する認証テーブル１６を作成し、（ｄ）さらにＬＡＮスイッチ１１はＰＣ３１からＰＣ３３へのパケットを受信すると、パケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブル１４（図２）を作成し、このとき前記ホストテーブル１４の中に前記始点ＩＰアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該パケットの受信ポートで且つ該パケットの始点ＩＰアドレスのＰＣにユーザ名とパスワードを要求するとともに、ユーザ名とパスワードが返されるのを待って、前記認証テーブル１６の中の前記始点ＩＰアドレスに該当する連絡先メールアドレスにホストテーブル１４の書き換え要求が発生した旨を伝えるメッセージ（本メッセージの中にＰＣから返されたユーザ名を情報として入れる。）を送り、さらに予め認証テーブル１６に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）は、ホストテーブル１４のエントリ書き換えを中止するとともに該パケットを廃棄し、予め認証テーブル１６に登録されているユーザ名とパスワードが得られた場合は、終点ＩＰアドレスをキーにホストテーブル１４を参照し、該当エントリが有る場合は、該当ポートにパケットを出力し、該当エントリが無い場合は、ルーティングテーブル（図示無し）およびＡＲＰテーブル（図示無し）を参照してネクストホップを決め、該当するホストテーブル１４のエントリを新規に作成して、該当ポートにパケットを出力することを特徴とするＬＡＮスイッチネットワークシステムの管理方法を提供する。

【００１４】上記第１の観点によるＬＡＮスイッチネットワークシステムの管理方法では、ＰＣ３１はポート２１から他のポートに移動した場合でも移動前と同様の通信を自動的に再開することができるが、その際、ＬＡＮスイッチ１１から予め登録したユーザ名とパスワードの入力を求められるため、そのパスワードを知っているＰＣ３１以外がＰＣ３１を装って盗聴したり、なりすましたりすることが出来なくなる。またＰＣ３２がＰＣ３１のＩＰアドレスを誤って設定、ポート２２に接続してしまった場合でも、ＰＣ３１およびＬＡＮスイッチ１１の管理者にその旨を伝えるメッセージ（本メッセージの中にＰＣ３２のユーザ名が入れられている）が送られるので、ＰＣ３１のユーザやＬＡＮスイッチ１１の管理者は容易に障害原因の切り分け（解析）を行うことができ、迅速な回復処理が可能になる。

【００１５】第２の観点では、本発明は、（ａ）各ポート２１～２５との間でパケットの送受信を行う通信処理手段１２と、（ｂ）前記通信処理手段１２から渡されたパケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブル１４（図２）を作成し、このとき前記ホストテーブル１４の中に前記始点ＩＰアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、書き換えて（新規作成も含む）良いか認証処理手段１５に問い合わせ、その結果、書き換え禁止の通知を受けた場合は、前記ホストテーブル１４のエントリ書き換えを中止するとともに該パケットを廃棄し、書き換え許可の通知を受けた場合は、終点ＩＰアドレスをキーに前記ホストテーブル１４を参照し、該当エントリが有る場合は、該当ポートへのパケット出力を前記通信処理手段１２に指示し、該当エントリが無い場合は、ルーティングテーブル（図示無し）およびＡＲＰテーブル（図示無し）を参照してネクストホップを決め、前記ホストテーブル１４に該当するエントリを新規に作成して、該当ポートへのパケット出力を前記通信処理手段１２に指示する中継処理手段１３と、（ｃ）予め管理端末（図示無し）等を介して入力された各ＰＣ３１～３４のＩＰアドレス、ユーザ名、パスワード、連絡先メールアドレス等を登録して認証テーブル１６を作成し、前記中継処理手段１３から指示されると、指示されたＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求するメッセージを作成して、該パケットの受信ポートへの送出を前記通信処理手段１２に指示するとともに、ユーザ名とパスワードが返されるのを待って、前記認証テーブル１６の中の前記ＩＰアドレスに該当する連絡先メールアドレスにホストテーブル１４のエントリ書き換え要求が発生した旨を伝えるメッセージ（本メッセージの中にＰＣから返されたユーザ名を情報として入れる）を作成して前記

通信処理手段１２に送出を指示し、さらに予め認証テーブル１６に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）は、前記ホストテーブル１４のエントリの書き換え禁止を前記中継処理手段１３に通知し、予め認証テーブル１６に登録されているユーザ名とパスワードが得られた場合は、前記ホストテーブル１４のエントリの書き換え許可を前記中継処理手段１３に通知する認証処理手段１５とを具備したことを特徴とするＬＡＮスイッチ１１を提供する。

【００１６】上記第２の観点によるＬＡＮスイッチ１１によれば、上記第１の観点のＬＡＮスイッチネットワークシステムの管理方法を好適に実施できるようになる。

【００１７】第３の観点では、本発明は、上記構成のＬＡＮスイッチ１１において、前記認証処理手段１５は、前記中継処理手段１３から指示されたホストテーブル１４のエントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求するメッセージを作成して、該パケットの受信ポートへの送出を前記通信処理手段１２に指示し、予め認証テーブル１６に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）は、前記ホストテーブル１４のエントリの書き換え禁止を前記中継処理手段１３に通知するだけでなく、該パケットを受信したポートの切り離しや該ポートから受信する全てのパケットの廃棄を前記中継処理手段１３に指示することを特徴とするＬＡＮスイッチ１１を提供する。

【００１８】上記第３の観点によるＬＡＮスイッチ１１によれば、ＩＰアドレス等の設定ミスや悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすまして通信を行おうとすることによるユーザ名とパスワードの入力要求の繰り返しのトラヒック負荷を減らすことができる。

【００１９】第４の観点では、本発明は、上記構成のＬＡＮスイッチ１１において、前記認証処理手段１５は、前記中継処理手段１３から指示されたホストテーブル１４のエントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求するメッセージを作成して、該パケットの受信ポートへの送出を前記通信処理手段１２に指示し、予め認証テーブル１６に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）は、前記ホストテーブル１４のエントリの書き換え禁止を前記中継処理手段１３に通知するだけでなく、該パケットの始点ＩＰアドレスと同一ＶＬＡＮに属す全てのＰＣのユーザに、ＩＰアドレス等の設定ミスや悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすましの通信を行おうとしている可能性があることを警告するメッセージを作成して、前記通信処理手段１２に指示して送出させることを特徴とするＬＡＮスイッチ１１を提供する。

【００２０】また、第４の観点の別の側面として、本発明は、上記構成のＬＡＮスイッチ１１において、前記認証処理手段１５は、前記中継処理手段１３から指示されたホストテーブル１４のエントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求するメッセージを作成して、該パケットの受信ポートへの出力を前記通信処理手段１２に指示し、予め認証テーブル１６に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）のみ、前記認証テーブル１６の中の前記始点ＩＰアドレスに該当する連絡先メールアドレスにホストテーブル１４の書き換え失敗が発生した旨を伝えるメッセージを作成して、前記通信処理手段１２に指示して送出させることを特徴とするＬＡＮスイッチ１１を提供する。

【００２１】上記第４の観点による前者のＬＡＮスイッチ１１によれば、ＩＰアドレス等の設定ミスや悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすましの通信を行おうとしていることを、当事者だけでなく、その後同じ事が起きる可能性があるユーザにも事前に警告を発することができる。

【００２２】また上記第４の観点による後者のＬＡＮスイッチ１１によれば、書き換え成功時（真正なユーザが正常な使用範囲で通信している場合）に真正なユーザに送られてくるメールを無くしてトラヒック量を減らすとともに、書き換えに失敗する場合のみ、その旨を伝えることによって、より迅速な障害原因の切り分け（解析）および回復処理が可能となる。

【００２３】第５の観点では、本発明は、上記構成のＬＡＮスイッチ１１において、前記認証処理手段１５は、ホストテーブル１４のエントリの新規作成時や書き換え時ではなく、各エントリについて定期的にユーザ名とパスワードの問い合わせを行うことを特徴とするＬＡＮスイッチ１１を提供する。

【００２４】上記第５の観点によるＬＡＮスイッチ１１によれば、パケットを受信するのみで自ら発信を行わないＰＣについても、ＩＰアドレス等の設定ミスをしていないか、悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすましの通信を行っていないかチェックすることができる。

【００２５】また上記第５の観点によるＬＡＮスイッチによれば、ポート接続ミス・ＩＰアドレス設定ミス等や、悪意のユーザが、それまで真正なユーザのＰＣが接続していたポートに、その真正なユーザのＩＰアドレスを設定してＰＣを接続し、盗聴やなりすましの通信を行っていないかチェックすることができる。

【００２６】第６の観点では、本発明は、上記構成のＬＡＮスイッチ１１において、前記中継処理手段１３は、受信パケットの始点ＩＰアドレスに該当するホストテーブル１４のエントリの新規作成時や書き換えが発生した場合に、それを書き換えて良いか前記認証処理手段１５に問い合わせるだけでなく、受信パケットの終点ＩＰア

ドレスについても同様に、該当するホストテーブル１４のエントリの新規作成時や書き換えが発生した場合に、それを書き換えて良いか前記認証処理手段１５に問い合わせることを特徴とするＬＡＮスイッチ１１を提供する。

【００２７】上記第６の観点によるＬＡＮスイッチ１１によれば、パケットを受信するのみで自ら発信を行わないＰＣについても、ＩＰアドレス等の設定ミスをしていないか、悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすましの通信を行っていないかチェックすることができる。

【００２８】また上記第６の観点によるＬＡＮスイッチによれば、ポート接続ミス・ＩＰアドレス設定ミス等や、悪意のユーザが、それまで真正なユーザのＰＣが接続していたポートに、その真正なユーザのＩＰアドレスを設定してＰＣを接続し、盗聴やなりすましの通信を行っていないかチェックすることができる。

【００２９】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照しながら詳細に説明する。なお、これにより本発明が限定されるものではない。

【００３０】図１は、本発明の第１の実施形態である通信ネットワークシステムの管理方法を実施するＬＡＮスイッチの構成、および当該ＬＡＮスイッチが適用されるＩＰサブネットベースＶＬＡＮの一例を示す概念図である。また、図２および図３は、本実施の形態のＬＡＮスイッチにて用いられる各種制御情報の一例を示す概念図、図４、図５および図６は、本実施の形態の通信ネットワークシステムの管理方法およびＬＡＮスイッチの作用の一例を示すフローチャートである。

【００３１】本実施の形態のＬＡＮスイッチ１１は、受信したパケット（通信情報）から学習して作成した図２のようなホストテーブル１４に基づき各ポート２１～２５間のパケットの中継を行うことにより、ＰＣ３１～３４の間の通信を実現するものであり、通信処理手段１２と、中継処理手段１３と、認証処理手段１５とから構成される。

【００３２】前記通信処理手段１２は、各ポート２１～２５との間でパケットの送受信を行う手段であり、例えばＣＰＵ、ＡＳＩＣ、ＲＡＭ、ＲＯＭ等の電子デバイスで構成される。

【００３３】前記中継処理手段１３は、ホストテーブル１４に基づき各ポート２１～２５間のパケットの中継を行う手段であり、例えばＣＰＵ、ＡＳＩＣ、ＲＡＭ、ＲＯＭ等の電子デバイスで構成される。

【００３４】図２に例示されるように、ホストテーブル１４は、始点ＩＰアドレス１４ａ、始点ＭＡＣアドレス１４ｂ、終点ＭＡＣアドレス１４ｃ、ポート番号１４ｄ、当該ポートが帰属するＶＬＡＮ等のネットワークを示す帰属ネットワーク１４ｅ、等の情報が対応付けられて格納されている。

【００３５】前記認証処理手段１５は、ホストテーブル１４の書き換え可不可の判定を行う手段であり、例えばＣＰＵ、ＡＳＩＣ、ＲＡＭ、ＲＯＭ等の電子デバイスで構成される。書き換え可不可の判定の基となる情報は認証テーブル１６（後述）に予め登録、保持している。

【００３６】図３は、本実施の形態のＬＡＮスイッチ１１にて用いられる認証テーブル１６の構成図である。認証テーブル１６には、ＰＣ３１～３４のＩＰアドレス１６ａと、そのＰＣを使用しているユーザ名１６ｂ、パスワード１６ｃ、連絡先メールアドレス１６ｄが予めコンソール端末（図示無し）等を介して登録されている。

【００３７】先ず、ＰＣ３１からＰＣ３３に通信する場合の動作について説明する。

【００３８】図４は、ＰＣ３１からＰＣ３３に通信する場合の本実施の形態のＬＡＮスイッチ１１および通信ネットワークシステムの管理方法の動作の一例を示すフローチャートである。

【００３９】なお各ＰＣ３１～３４はＬＡＮスイッチ１１に予めＩＰアドレスとそのユーザ名、パスワード、連絡先メールアドレスを登録し、ＬＡＮスイッチ１１の管理者も同様にＬＡＮスイッチ１１に予め連絡先メールアドレスを登録し、ＬＡＮスイッチ１１は前記ＰＣ３１～３４および前記ＬＡＮスイッチ１１の管理者の情報を登録する認証テーブル１６を作成してあるものとする。

【００４０】ＰＣ３１は、ＰＣ３３宛のパケットを作成してポート２１に送出する（ステップ１０１）。

【００４１】ＬＡＮスイッチ１１の通信処理手段１２は、前記パケットをポート２１から受信処理して中継処理手段１３に渡す（ステップ１０２）。

【００４２】中継処理手段１３は、受信パケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブル１４を作成する。このときホストテーブル１４の中に前記始点ＩＰアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該エントリを書き換えて（新規作成も含む）良いか認証処理手段１５に問い合わせる（ステップ１０３）。書き換える必要（新規作成も含む）が無い場合はステップ１１０に進む。本ケースは通信開始の１パケット目のケースであり、新規作成するため次ステップに進むものとする。２パケット目以降のケースではステップ１１０に進む。

【００４３】認証処理手段１５は、ユーザ名とパスワードの入力要求メッセージ（メッセージＡと呼ぶ。）を作成して通信処理手段１２に送出を指示した後、一定時間待つ（ステップ１０４）。

【００４４】通信処理手段１２は、メッセージＡを該パケットの受信ポート（この場合、ポート２１）の該ＩＰアドレス宛に送出する（ステップ１０５）。

【００４５】通信処理手段１２は、メッセージＡの応答

メッセージ、すなわちユーザ名とパスワードの入力メッセージ（メッセージＢと呼ぶ。）をＰＣ３１から受信すると、受信処理して認証処理手段１５に渡す（ステップ１０６）。

【００４６】認証処理手段１５は、メッセージＢに格納されているＩＰアドレス、ユーザ名、パスワードと、認証テーブル１６に書かれているＩＰアドレス１６ａ、ユーザ名１６ｂ、パスワード１６ｃを比較して一致することを確認した後、認証テーブル１６の該当エントリに登録されている連絡先メールアドレス１６ｄにホストテーブル１４の書き換え要求が発生した旨を伝えるメッセージ（メッセージＣと呼ぶ。メッセージＣの中にはメッセージＢに格納されているユーザ名を情報として入れる。）を作成して通信処理手段１２に送出を指示する（ステップ１０７）とともに、書き換え許可の旨を中継処理手段１３に通知する（ステップ１０９）。

【００４７】通信処理手段１２は、メッセージＣを該メールアドレス宛に送出する（ステップ１０８）。

【００４８】一方、中継処理手段１３は、認証処理手段１５から書き換え許可の旨の通知を受けると、ホストテーブル１４の該当エントリの書き換えを行い、次に終点ＩＰアドレスをキーにホストテーブル１４を参照し、該当エントリが有る場合は、該当ポートへのパケット出力を通信処理手段１２に指示し、該当エントリが無い場合は、ルーティングテーブル（図示無し）およびＡＲＰテーブル（図示無し）を参照してネクストホップを決め、該当するホストテーブル１４のエントリを新規に作成して、該当ポートへのパケット出力を通信処理手段１２に指示する（ステップ１１０）。

【００４９】通信処理手段１２は、該パケットを該当ポートに送出する（ステップ１１１）。

【００５０】以上により、ＰＣ３１からＰＣ３３への通信を開始することが出来る。

【００５１】次にＰＣ３１がポート２１からポート２５に移動した後、ＰＣ３３に通信する場合の動作について説明する。

【００５２】ＰＣ３１のＩＰアドレスに該当するエントリが既にホストテーブル１４にできている点が前述のケースと異なるが、動作は図４に示すフローチャートと同じ動きをする。

【００５３】ＰＣ３１は、ＰＣ３３宛のパケットを作成してポート２１に送出する（ステップ１０１）。

【００５４】ＬＡＮスイッチ１１の通信処理手段１２は、前記パケットを受信処理して中継処理手段１３に渡す（ステップ１０２）。

【００５５】中継処理手段１３は、受信パケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブル１４を作成する。このときホストテーブル１４の中に前記始点ＩＰアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該エントリを書き換えて（新規作成も含む）良いか認証処理手段１５に問い合わせる（ステップ１０３）。書き換える必要（新規作成も含む）が無い場合はステップ１１０に進む。本ケースは移動後の通信再開の１パケット目のケースであり、エントリの情報を書き換えるため次ステップに進むものとする。２パケット目以降のケースではステップ１１０に進む。

【００５６】認証処理手段１５は、ユーザ名とパスワードの入力要求メッセージ（メッセージＡと呼ぶ。）を作成して通信処理手段１２に送出を指示した後、一定時間待つ（ステップ１０４）。

【００５７】通信処理手段１２は、メッセージＡを該パケットの受信ポートの該ＩＰアドレス宛に送出する（ステップ１０５）。

【００５８】通信処理手段１２は、メッセージＡの応答メッセージ、すなわちユーザ名とパスワードの入力メッセージ（メッセージＢと呼ぶ。）を受信すると、受信処理して認証処理手段１５に渡す（ステップ１０６）。

【００５９】認証処理手段１５は、メッセージＢに格納されているＩＰアドレス、ユーザ名、パスワードと、認証テーブル１６に書かれているＩＰアドレス１６ａ、ユーザ名１６ｂ、パスワード１６ｃを比較して一致することを確認した後、認証テーブル１６の該当エントリに登録されている連絡先メールアドレス１６ｄにホストテーブル１４の書き換え要求が発生した旨を伝えるメッセージ（メッセージＣと呼ぶ。メッセージＣの中にはメッセージＢに格納されているユーザ名を情報として入れる。）を作成して通信処理手段１２に送出を指示する（ステップ１０７）とともに、書き換え許可の旨を中継処理手段１３に通知する（ステップ１０９）。

【００６０】通信処理手段１２は、メッセージＣを該メールアドレス宛に送出する（ステップ１０８）。

【００６１】一方、中継処理手段１３は、認証処理手段１５から書き換え許可の旨の通知を受けると、ホストテーブル１４の該当エントリの書き換えを行い、次に終点ＩＰアドレスをキーにホストテーブル１４を参照し、該当エントリが有る場合は、該当ポートへのパケット出力を通信処理手段１２に指示し、該当エントリが無い場合は、ルーティングテーブル（図示無し）およびＡＲＰテーブル（図示無し）を参照してネクストホップを決め、該当するホストテーブル１４のエントリを新規に作成して、該当ポートへのパケット出力を通信処理手段１２に指示する（ステップ１１０）。

【００６２】通信処理手段１２は、該パケットを該当ポート（この場合、ポート２５）に送出する（ステップ１１１）。

【００６３】以上により、ＰＣ３１はポート２１からポート２５へ移動後も、ＰＣ３３との通信を自動的に再開することが出来る。

【００６４】次にＰＣ３２がＰＣ３１のＩＰアドレスを誤って設定、ポート２２に接続してしまい、ＰＣ３３との通信を開始した場合の動作について説明する。

【００６５】図５は、ＰＣ３２がＰＣ３１のＩＰアドレスを誤って設定、ポート２２に接続してしまい、ＰＣ３３との通信を開始した場合における、本実施の形態のＬＡＮスイッチ１１および通信ネットワークシステムの管理方法の動作の一例を示すフローチャートである。

【００６６】ＰＣ３２は、ＰＣ３３宛のパケットを作成してポート２１に送出する（ステップ１２１）。

【００６７】ＬＡＮスイッチ１１の通信処理手段１２は、前記パケットを受信処理して中継処理手段１３に渡す（ステップ１０２）。

【００６８】中継処理手段１３は、受信パケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブル１４を作成する。このときホストテーブル１４の中に前記始点ＩＰアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該エントリを書き換えて（新規作成も含む）良いか認証処理手段１５に問い合わせる（ステップ１０３）。書き換える必要（新規作成も含む）が無い場合はステップ１１０に進む。本ケースはＰＣ３２がＰＣ３１のＩＰアドレスを誤って設定、ポート２２に接続してしまい、ＰＣ３３との通信を開始した１パケット目のケースであり、エントリの情報を書き換えるため次ステップに進むものとする。なお本ケースでは結果としてエントリの情報の書き換えに失敗するため、２パケット目以降のケースも次ステップに進むことになる。

【００６９】認証処理手段１５は、ユーザ名とパスワードの入力要求メッセージ（メッセージＡと呼ぶ。）を作成して通信処理手段１２に送出を指示した後、一定時間待つ（ステップ１０４）。

【００７０】通信処理手段１２は、メッセージＡを該パケットの受信ポート（この場合、ポート２２）の該ＩＰアドレス宛に送出する（ステップ１０５）。

【００７１】通信処理手段１２は、メッセージＡの応答メッセージ、すなわちユーザ名とパスワードの入力メッセージ（メッセージＢと呼ぶ。）を受信すると、受信処理して認証処理手段１５に渡す（ステップ１０６）。

【００７２】認証処理手段１５は、メッセージＢに格納されているＩＰアドレス、ユーザ名、パスワードと、認証テーブル１６に書かれているＩＰアドレス１６ａ、ユーザ名１６ｂ、パスワード１６ｃを比較して一致していないことを確認した後、認証テーブル１６の該当エントリに登録されている連絡先メールアドレス１６ｄにホストテーブル１４の書き換え要求が発生した旨を伝えるメッセージ（メッセージＣと呼ぶ。メッセージＣの中にはメッセージＢに格納されているユーザ名を情報として入れる。）を作成して通信処理手段１２に送出を指示する（ステップ１０８）とともに、書き換え禁止の旨を中継処理手段１３に通知する（ステップ１２２）。

【００７３】通信処理手段１２は、メッセージＣを該メールアドレス宛に送出する（この場合、メッセージＣは、ＰＣ３２において謝って設定されたＩＰアドレスの真正の所有者であるＰＣ３１宛にメッセージＣが送られる。）（ステップ１０８）。

【００７４】一方、中継処理手段１３は、認証処理手段１５から書き換え禁止の旨の通知を受けると、ホストテーブル１４の該当エントリの書き換えを中止し、該パケットを廃棄する（ステップ１２３）。

【００７５】以上により、ＰＣ３２がＰＣ３１のＩＰアドレスを誤って設定、ポート２２に接続してしまった場合でも、真正のＰＣ３１およびＬＡＮスイッチ１１の管理者にその旨を伝えるメッセージ（本メッセージの中に誤設定操作を行ったＰＣ３２のユーザ名が入れられている）が送られるので、ＰＣ３１のユーザやＬＡＮスイッチ１１の管理者は容易に障害原因の切り分けを行うことができ、迅速な回復処理が可能となる。

【００７６】次に悪意のユーザのＰＣ３５がＰＣ３１のＩＰアドレスを設定、ポート２５に接続し、ＰＣ３３との通信を開始した場合の動作について説明する。

【００７７】図６は、悪意のユーザのＰＣ３５がＰＣ３１のＩＰアドレスを設定、ポート２５に接続し、ＰＣ３３との通信を開始した場合における、本実施の形態のＬＡＮスイッチ１１および通信ネットワークシステムの管理方法の動作の一例を示すフローチャートである。

【００７８】ＰＣ３５は、ＰＣ３３宛のパケットを作成してポート２５に送出する（ステップ１３１）。

【００７９】ＬＡＮスイッチ１１の通信処理手段１２は、前記パケットを受信処理して中継処理手段１３に渡す（ステップ１０２）。

【００８０】中継処理手段１３は、受信パケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブル１４を作成する。このときホストテーブル１４の中に前記始点ＩＰアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該エントリを書き換えて（新規作成も含む）良いか認証処理手段１５に問い合わせる（ステップ１０３）。書き換える必要（新規作成も含む）が無い場合はステップ１１０に進む。本ケースは悪意のユーザのＰＣ３５がＰＣ３１のＩＰアドレスを設定、ポート２５に接続し、ＰＣ３３との通信を開始した１パケット目のケースであり、エントリの情報を書き換えるため次ステップに進むものとする。なお本ケースでは結果としてエントリの情報の書き換えに失敗するため、２パケット目以降のケースも次ステップに進むことになる。

【００８１】認証処理手段１５は、ユーザ名とパスワードの入力要求メッセージ（メッセージＡと呼ぶ。）を作

成して通信処理手段１２に送出を指示した後、一定時間待つ（ステップ１０４）。

【００８２】通信処理手段１２は、メッセージＡを該パケットの受信ポート（この場合、ポート２５）の該ＩＰアドレス宛に送出する（ステップ１０５）。

【００８３】通信処理手段１２は、メッセージＡの応答メッセージ、すなわちユーザ名とパスワードの入力メッセージ（メッセージＢと呼ぶ。）を受信すると、受信処理して認証処理手段１５に渡す（ステップ１０６）。

【００８４】認証処理手段１５は、メッセージＢに格納されているＩＰアドレス、ユーザ名、パスワードと、認証テーブル１６に書かれているＩＰアドレス１６ａ、ユーザ名１６ｂ、パスワード１６ｃを比較して一致していないことを確認した後、認証テーブル１６の該当エントリに登録されている連絡先メールアドレス１６ｄにホストテーブル１４の書き換え要求が発生した旨を伝えるメッセージ（メッセージＣと呼ぶ。メッセージＣの中にはメッセージＢに格納されているユーザ名を情報として入れる。メッセージＢにユーザ名が入れられてない場合や一定時間内にメッセージＢが送られてこなかった場合はその旨を伝える情報を入れる。）を作成して通信処理手段１２に送出を指示する（ステップ１２２）とともに、書き換え禁止の旨を中継処理手段１３に通知する（ステップ１０９）。

【００８５】通信処理手段１２は、メッセージＣを該メールアドレス宛に送出する（この場合、メッセージＣは、パケットの送信元のＰＣ３５ではなく、真正のユーザであるＰＣ３１に届く）（ステップ１０８）。

【００８６】一方、中継処理手段１３は、認証処理手段１５から書き換え禁止の旨の通知を受けると、ホストテーブル１４の該当エントリの書き換えを中止し、該パケットを廃棄する（ステップ１２３）。

【００８７】また、メッセージＣを受け取ったシステムの管理者は、メッセージＣに格納されている情報に基づいて事態を把握し、対策をとることができる。

【００８８】以上により、悪意のユーザのＰＣ３５がＰＣ３１のＩＰアドレスを設定し、ポート２５に接続しても、ＰＣ３５は予めＰＣ３１がＬＡＮスイッチ１１に登録したユーザ名とパスワードの入力を求められ、それに正しく応えられないため、ホストテーブル１４の書き換えは行われず、したがってＰＣ３５がＰＣ３１を装って盗聴したり、なりすましたりすることを防ぐことができる。

【００８９】次に、第１の実施例とは別の実施例について説明する。

【００９０】第１の実施例ではＬＡＮスイッチ１１において、認証処理手段１５は、中継処理手段１３から指示されたホストテーブル１４のエントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求するメッセージＡを作成して、該パケットの受信ポートへの送出を通信処理手段１２に指示し、予め認証テーブル１６に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）は、前記ホストテーブル１４のエントリの書き換え禁止を前記中継処理手段１３に通知しているが、さらにそれに加えて該パケットを受信したポートの切り離し（閉塞）や該ポートから受信する全てのパケットの廃棄を前記中継処理手段１３に指示するようにしても良い。以上により、ＩＰアドレス等の設定ミスや悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすまして通信を行おうとすることによるユーザ名とパスワードの入力要求の繰り返しのトラヒック負荷を減らすことができる。

【００９１】また、第１の実施例ではＬＡＮスイッチ１１において、認証処理手段１５は、中継処理手段１３から指示されたホストテーブル１４のエントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求するメッセージＡを作成して、該パケットの受信ポートへの送出を通信処理手段１２に指示し、予め認証テーブル１６に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）は、前記ホストテーブル１４のエントリの書き換え禁止を前記中継処理手段１３に通知しているが、さらにそれに加えて該パケットの始点ＩＰアドレスと同一ＶＬＡＮに属す全てのＰＣのユーザに、ＩＰアドレス等の設定ミスや悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすましの通信を行おうとしている可能性があることを警告するメッセージを作成して、前記通信処理手段１２に指示して送出させても良い。以上により、ＩＰアドレス等の設定ミスや悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすましの通信を行おうとしていることを、当事者だけでなく、その後同じ事が起きる可能性があるユーザにも事前に警告を発することができる。

【００９２】また、第１の実施例ではＬＡＮスイッチ１１において、認証処理手段１５は、ホストテーブル１４のエントリの新規作成や書き換えが発生し、中継処理手段１３から書き換え（新規作成を含む）て良いか問い合わせを受けた時に該エントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求しているが、定期的に各エントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求して真正のユーザか否かを確認するユーザ認証を行っても良い。以上により、パケットを受信するのみで自ら発信を行わないＰＣについても、ＩＰアドレス等の設定ミスをしていないか、悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすましの通信を行っていないかチェックすることができる。

【００９３】また、第１の実施例ではＬＡＮスイッチ１１において、中継処理手段１３は、受信パケットの始点ＩＰアドレスに該当するホストテーブル１４のエントリの新規作成時や書き換えが発生した場合に、それを書き

換えて良いか認証処理手段１５に問い合わせるだけでなく、受信パケットの終点ＩＰアドレスについても同様に、該当するホストテーブル１４のエントリの新規作成時や書き換えが発生した場合に、それを書き換えて良いか前記認証処理手段１５に問い合わせ、書き換え許可がおりた場合のみ該エントリの書き換えを行うようにしても良い。以上により、パケットを受信するのみで自ら発信を行わないＰＣについても、ＩＰアドレス等の設定ミスをしていないか、悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすましの通信を行っていないかチェックすることができる。

【００９４】また、第１の実施例ではＩＰサブネットベースＶＬＡＮの例を用いて説明しているが、ポートベースＶＬＡＮ、ＭＡＣアドレスベースＶＬＡＮ、Layer3プロトコルベースＶＬＡＮ等の他の形式のＶＬＡＮでも同様である。

【００９５】以上のように、本発明の各実施の形態の通信ネットワークの管理方法およびＬＡＮスイッチによれば、悪意のユーザによる盗聴やなりすましを防ぐことができ、通信ネットワークシステムのセキュリティが向上する。

【００９６】また、ユーザ認証にて得られたユーザ名等の情報を真正のユーザやシステムの管理者にメールで通知することにより、ＩＰアドレス等の設定ミスによる障害原因を容易に切り分けられるようになり、迅速な回復処理が可能になる。

【００９７】上記した特許請求の範囲に記載された以外の本発明の特徴を列挙すれば以下の通りである。

【００９８】すなわち、

＜１＞　ＬＡＮスイッチで構成する通信ネットワークシステムの管理方法であって、（ａ）各ＰＣはＬＡＮスイッチに予めＩＰアドレスとそのユーザ名、パスワード、連絡先メールアドレスを登録し、（ｂ）ＬＡＮスイッチの管理者も同様にＬＡＮスイッチに予め連絡先メールアドレスを登録し、（ｃ）ＬＡＮスイッチは前記ＰＣおよび前記ＬＡＮスイッチの管理者の情報を登録する認証テーブルを作成し、（ｄ）さらにＬＡＮスイッチは各ＰＣ間の通信のパケットを受信すると、該パケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブルを作成し、このとき前記ホストテーブルの中に前記始点ＩＰアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該パケットの受信ポートで且つ該パケットの始点ＩＰアドレスのＰＣにユーザ名とパスワードを要求するとともに、ユーザ名とパスワードが返されるのを待って、前記ホストテーブルの書き換え要求が発生した旨を伝えるメッセージを作成し、該メッセージの中にＰＣから返されたユーザ名を情報として入れ、前記認証テーブルの中の前記始点ＩＰアドレスに該当する連絡先メールアドレスに送り、さらに予め前記認証テーブルに登録されているユーザ名とパスワードが得られなかった場合や一定時間内に応答が返されなかった場合は、前記ホストテーブルのエントリ書き換えを中止するとともに該パケットを廃棄し、予め前記認証テーブルに登録されているユーザ名とパスワードが得られた場合は、終点ＩＰアドレスをキーに前記ホストテーブルを参照し、該当エントリが有る場合は、該当ポートにパケットを出力し、該当エントリが無い場合は、該当するホストテーブルのエントリを新規に作成して、該当ポートにパケットを出力することを特徴とする通信ネットワークシステムの管理方法。

【００９９】＜２＞　前記＜１＞記載の通信ネットワークシステムの管理方法において、ＬＡＮスイッチは、予め前記認証テーブルに登録されているユーザ名とパスワードが得られなかった場合や一定時間内に応答が返されなかった場合に、前記ホストテーブルのエントリ書き換えを中止し、該パケットを廃棄することに加えて、さらに該パケットを受信したポートの切り離しや該ポートから受信する全てのパケット廃棄を行うことを特徴とする通信ネットワークシステムの管理方法。

【０１００】＜３＞　前記＜１＞記載の通信ネットワークシステムの管理方法において、ＬＡＮスイッチは、予め前記認証テーブルに登録されているユーザ名とパスワードが得られなかった場合や一定時間内に応答が返されなかった場合に、前記ホストテーブルのエントリ書き換えを中止し、該パケットを廃棄することに加えて、さらに該パケットの始点ＩＰアドレスと同一ＶＬＡＮに属す全てのＰＣのユーザに、ＩＰアドレス等の設定ミスや悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすましの通信を行おうとしている可能性があることを警告するメッセージを作成して送ることを特徴とする通信ネットワークシステムの管理方法。

【０１０１】＜４＞　前記＜１＞記載の通信ネットワークシステムの管理方法において、ＬＡＮスイッチは、ホストテーブルのエントリ新規作成時や書き換えが発生した場合に該エントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求することに加えて、さらに定期的に各エントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求することを特徴とする通信ネットワークシステムの管理方法。

【０１０２】＜５＞　前記＜１＞記載の通信ネットワークシステムの管理方法において、ＬＡＮスイッチは、受信パケットの始点ＩＰアドレスに該当するホストテーブルのエントリの新規作成時や書き換えが発生した場合に該エントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求することに加えて、さらに該パケットの終点ＩＰアドレスに該当するホストテーブルのエントリの新規作成時や書き換えが発生した場合に該エントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求し、始点ＩＰアドレスと同様に終点ＩＰアドレスにつ

いても、予め認証テーブルに登録されているユーザ名とパスワードが得られた場合のみ該エントリの書き換えを行うことを特徴とする通信ネットワークシステムの管理方法。

【０１０３】＜６＞　（ａ）各ポートとの間でパケットの送受信を行う通信処理手段と、（ｂ）前記通信処理手段から渡されたパケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブルを作成し、このとき前記ホストテーブルの中に前記始点ＩＰアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、新規作成または書き換えて良いか認証処理手段に問い合わせ、その結果、書き換え禁止の通知を受けた場合は、前記ホストテーブルのエントリ書き換えを中止するとともに該パケットを廃棄し、書き換え許可の通知を受けた場合は、終点ＩＰアドレスをキーに前記ホストテーブルを参照し、該当エントリが有る場合は、該当ポートへのパケット出力を前記通信処理手段に指示し、該当エントリが無い場合は、前記ホストテーブルに該当するエントリを新規に作成して、該当ポートへのパケット出力を前記通信処理手段に指示する中継処理手段と、（ｃ）予め管理端末等を介して入力された各ＰＣのＩＰアドレス、ユーザ名、パスワード、連絡先メールアドレス等を登録して認証テーブルを作成し、前記中継処理手段から指示されると、指示されたＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求するメッセージを作成して、前記パケットの受信ポートへの送出を前記通信処理手段に指示するとともに、ユーザ名とパスワードが返されるのを待って、前記認証テーブルの中の前記ＩＰアドレスに該当する連絡先メールアドレスに前記ホストテーブルのエントリ書き換え要求が発生した旨を伝えるメッセージを作成し、該メッセージの中にＰＣから返されたユーザ名を情報として入れ、前記通信処理手段に送出を指示し、さらに予め前記認証テーブルに登録されているユーザ名とパスワードが得られなかった場合や一定時間内に応答が返されなかった場合は、前記ホストテーブルのエントリの書き換え禁止を前記中継処理手段に通知し、予め認証テーブルに登録されているユーザ名とパスワードが得られた場合は、前記ホストテーブルのエントリの書き換え許可を前記中継処理手段に通知する認証処理手段とを具備したことを特徴とするＬＡＮスイッチ。

【０１０４】＜７＞　ＬＡＮスイッチで構成する通信ネットワークシステムの管理方法であって、（ａ）各ＰＣはＬＡＮスイッチに予めＭＡＣアドレスとそのユーザ名、パスワード、連絡先メールアドレスを登録し、（ｂ）ＬＡＮスイッチの管理者も同様にＬＡＮスイッチに予め連絡先メールアドレスを登録し、（ｃ）ＬＡＮスイッチは前記ＰＣおよび前記ＬＡＮスイッチの管理者の情報を登録する認証テーブルを作成し、（ｄ）さらにＬＡＮスイッチは各ＰＣ間の通信のパケットを受信すると、該パケットの始点ＭＡＣアドレスを学習してホストテーブルを作成し、このとき前記ホストテーブルの中に前記始点ＭＡＣアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該パケットの受信ポートで且つ該パケットの始点ＭＡＣアドレスのＰＣにユーザ名とパスワードを要求するとともに、ユーザ名とパスワードが返されるのを待って、前記ホストテーブルの書き換え要求が発生した旨を伝えるメッセージを作成し、該メッセージの中にＰＣから返されたユーザ名を情報として入れ、前記認証テーブルの中の前記始点ＭＡＣアドレスに該当する連絡先メールアドレスに送り、さらに予め前記認証テーブルに登録されているユーザ名とパスワードが得られなかった場合や一定時間内に応答が返されなかった場合は、前記ホストテーブルのエントリ書き換えを中止するとともに該パケットを廃棄し、予め前記認証テーブルに登録されているユーザ名とパスワードが得られた場合は、終点ＭＡＣアドレスをキーに前記ホストテーブルを参照し、該当エントリが有る場合は、該当ポートにパケットを出力し、該当エントリが無い場合は、該当するホストテーブルのエントリを新規に作成して、該当ポートにパケットを出力することを特徴とする通信ネットワークシステムの管理方法。

【０１０５】以上本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【０１０６】

【発明の効果】本発明の通信ネットワークシステムの管理方法によれば、論理的あるいは物理的なネットワークアドレス等の設定ミスによる通信不良の防止や通信不良の原因解析および回復操作の迅速化が可能になる、という効果が得られる。

【０１０７】また、本発明の通信ネットワークシステムの管理方法によれば、悪意のユーザによる盗聴やなりすましを防ぐことで通信ネットワークのセキュリティを向上させることができる、という効果が得られる。

【０１０８】本発明の情報中継装置によれば、論理的あるいは物理的なネットワークアドレス等の設定ミスによる通信不良の防止や通信不良の解析および回復操作の迅速化が可能になる、という効果が得られる。

【０１０９】また、本発明の情報中継装置によれば、悪意のユーザによる盗聴やなりすましを防ぐことで通信ネットワークシステムのセキュリティを向上させることができる、という効果が得られる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態である通信ネットワークシステムの管理方法を実施するＬＡＮスイッチの構成の一例を示す概念図である。

【図２】本発明の第１の実施形態である通信ネットワー

21

クシステムの管理方法を実施するＬＡＮスイッチにて用いられるホストテーブルの一例を示す概念図である。

【図３】本発明の第１の実施形態である通信ネットワークシステムの管理方法を実施するＬＡＮスイッチにて用いられる認証テーブルの一例を示す概念図である。

【図４】本発明の第１の実施形態である通信ネットワークシステムの管理方法を実施するＬＡＮスイッチの作用の一例を示すフローチャートである。

【図５】本発明の第１の実施形態である通信ネットワークシステムの管理方法を実施するＬＡＮスイッチの作用の一例を示すフローチャートである。

【図６】本発明の第１の実施形態である通信ネットワークシステムの管理方法を実施するＬＡＮスイッチの作用の一例を示すフローチャートである。

22

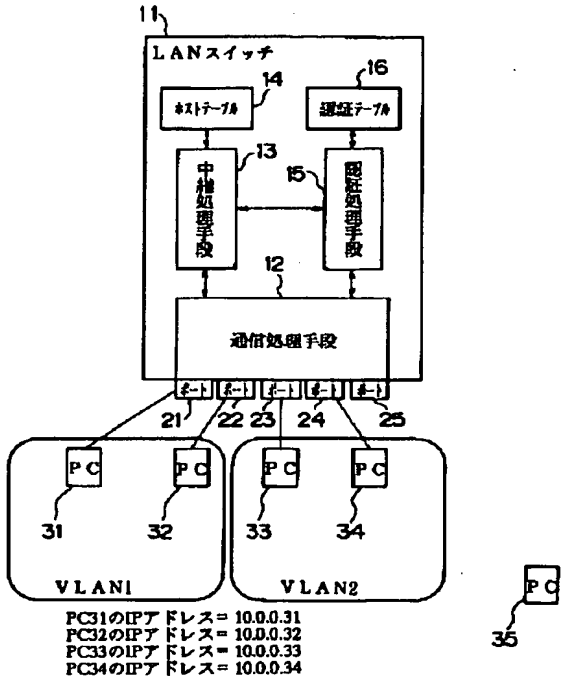
【図７】本発明の参考技術であるＩＰサブネットベースＶＬＡＮの一例を示す概念図である。

【符号の説明】

１１…ＬＡＮスイッチ（情報中継装置）、１２…通信処理手段（制御論理）、１３…中継処理手段（制御論理）、１４…ホストテーブル（制御テーブル）、１４ａ…始点ＩＰアドレス、１４ｂ…始点ＭＡＣアドレス、１４ｃ…終点ＭＡＣアドレス、１４ｄ…ポート番号、１４ｅ…帰属ネットワーク、１５…認証処理手段（制御論理）、１６…認証テーブル、１６ａ…ＩＰアドレス、１６ｂ…ユーザ名、１６ｃ…パスワード、１６ｄ…連絡先メールアドレス、２１～２５…ポート（入出力ポート）、３１～３４，３５…ＰＣ、Ａ，Ｂ，Ｃ…メッセージ。

【図１】

図　1




【図２】

図　2

14

ホストテーブル

| 14a 始点IPアドレス | 14b 始点MACアドレス | 14c 終点MACアドレス | 14d ポート番号 | 14e VLAN |
|---|---|---|---|---|
| 10.0.0.31 | 10:00:00:00:00:31 | 10:00:00:00:00:51 | 21 | 1 |
| 10.0.0.32 | 10:00:00:00:00:32 | 10:00:00:00:00:52 | 22 | 1 |
| 10.0.0.33 | 10:00:00:00:00:33 | 10:00:00:00:00:53 | 23 | 2 |
| 10.0.0.34 | 10:00:00:00:00:34 | 10:00:00:00:00:54 | 24 | 2 |

【図３】

図　3

16

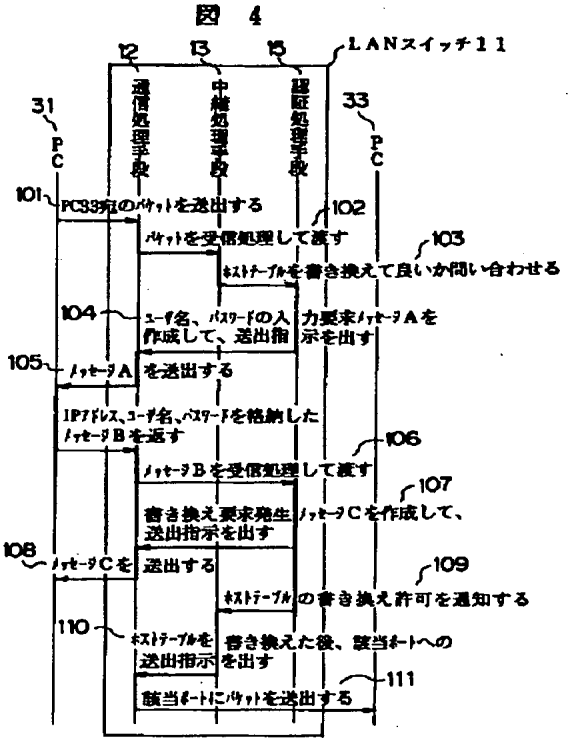
認証テーブル　16b　16c　16d

16a

| IPアドレス | ユーザ名 | Password | 連絡先メールアドレス |
|---|---|---|---|
| 10.0.0.31 | PC31 | pass31 | pc31@hitachi.co.jp, sella@hitachi.co.jp |
| 10.0.0.32 | PC32 | pass32 | pc32@hitachi.co.jp, sella@hitachi.co.jp |
| 10.0.0.33 | PC33 | pass33 | pc33@hitachi.co.jp, sella@hitachi.co.jp |
| 10.0.0.34 | PC34 | pass34 | pc34@hitachi.co.jp, sella@hitachi.co.jp |

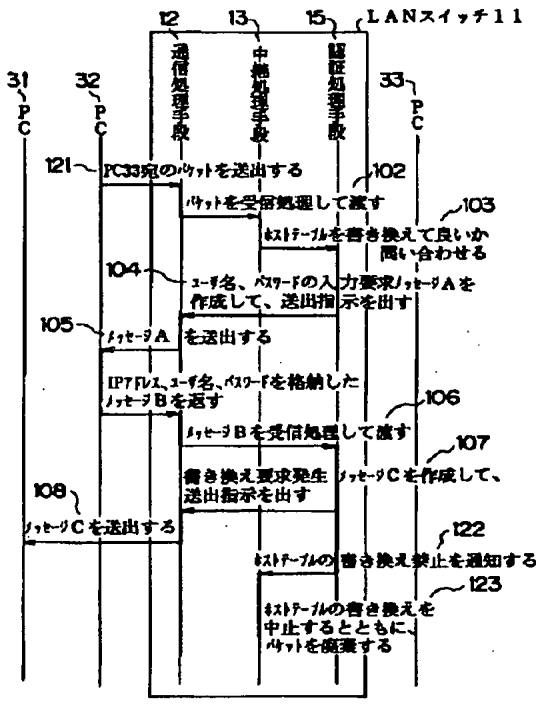
【図４】

図　4



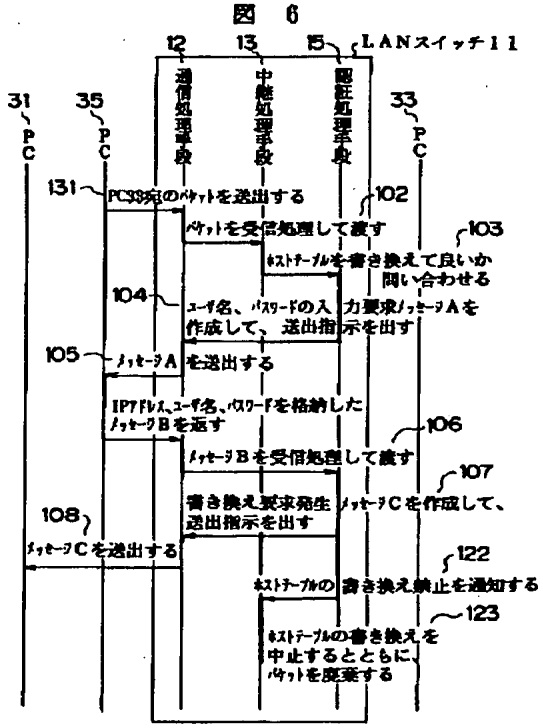

【図５】

図　5



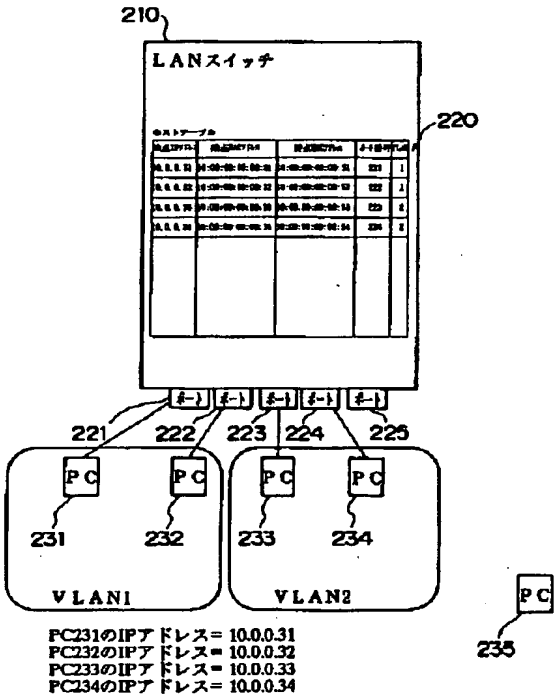

【図６】

図　6



【図7】

図　7




---

フロントページの続き

| (51)Int.Cl.[7] | 識別記号 | F I | ﾃｰﾏｺｰﾄﾞ(参考) |
|---|---|---|---|
| H04L 29/14 | | | |

Fターム(参考)　5J104 AA07 KA01 NA05 PA07
5K030 GA11 GA15 GA17 HC14 HD06
HD10 JT09 KA01 KA02 LB05
5K033 AA05 DA05 DB03 DB12 DB14
EC04
5K035 AA06 DD01 LL01
9A001 CC07 CC08 DD10 JJ18 JJ25
KZ56 LL03